Appendix A

Network Security Management
(Sample Security SOP)

This appendix provides a sample security SOP. It gives examples of specific guidance and procedures for ISS personnel in establishing their unit's SOP. Its intent is to provide minimum security for operating at the SECRET level in the systems high mode of operation. In this mode, all users must have a SECRET security clearance. C2 systems will be accredited to process and store SECRET data. The security guidelines and procedures for all information systems should be distributed through the chain of command down to the user level. Information systems include ABCS, Army Tactical Command and Control System (ATCCS), COTS, and components connected to the network. These guidelines and procedures may be incorporated, when appropriate, into existing unit SOPs. It should apply to all units and to all elements assigned, attached, or under the operational control of the issuing headquarters. The OPLANs and OPORDs should note the exceptions to the established SOP. This SOP applies to information systems and their components.

ISS POSITIONS

A-1. Commanders should select personnel for ISS positions who can provide assistance in implementing security procedures. These personnel must have the authority to enforce security policies, to include shutting down information systems if warranted by the seriousness of a security incident. Personnel selected should serve as the commander's focal point for all network security matters.

COMMANDERS

A-2. Commanders have the overall responsibility for network security. They will–

- Operate systems within their command IAW AR 380-19 and unit SOPs.
- Appoint an ISSM.
- Establish reasonable procedures to protect information systems and data from compromise, theft, or damage.
- Include ISS in the unit's training program.
- Use information systems for their intended purpose.
- Incorporate information systems requirements into unit contingency planning.

ISSM

A-3. At all levels of command, an ISSM is appointed to establish and implement the ISS program. These ISSMs are normally the deputy G6 and/or S6, and they –

- Develop the systems operational concept, security SOP, and security accreditation.
- Conduct individual systems risk assessment for operating their information systems.
- Conduct system-specific security training and awareness programs.

INTELLIGENCE OFFICER

A-4. The brigade intelligence officer (S2) identifies and assesses foreign intelligence threats to command assets. The S2–

- Administers the Personnel Security Program IAW AR 380-67.
- Ensures the Command Statement of Intelligence Interest registers the receipt of validated intelligence impacting on the integrity and reliability of the network (AR 381-19).
- Assists in identifying threat factors.
- Coordinates with national intelligence agencies.
- Evaluates security incidents and implements reporting procedures.

ISSO

A-5. The automation officer and/or systems integration technician in the G6/S6 signal office normally serve as the ISSO. He–

- Prepares, distributes, and maintains plans, instructions, guidance, and SOPs for C2 systems security.
- Ensures all systems have approved accreditation (operational or generic) to operate at the SECRET level in the systems high mode of operation IAW AR 380-19.
- Coordinates with the brigade S2 to ensure users have the required security investigations, clearances, authorizations, and the need-to-know.
- Establishes and implements a system for issuing, protecting, and changing system passwords.
- Implements ISS training and awareness and incorporates this training into the overall unit security and training programs.
- Monitors, reviews, and evaluates the security impact of changes and coordinates this with the ISSM.
- Directs threat and vulnerability assessments to help the commander properly analyze the risks to the information systems and interconnected systems.
- Provides guidance to ensure maximum protection against compromise and theft of sensitive information and prevents the misuse or misappropriation of information systems.

- Maintains an accurate inventory of all hardware and software throughout their units. Ensures this inventory is reconciled with the appropriate property book officer at least annually.
- Ensures the unit's contingency plans incorporate information systems requirements.
- Conducts periodic inspections and reviews to ensure compliance with this SOP and other policies in operations and security.
- Suspends operations partially or completely upon detection of actions that may affect security.
- Oversees the review of system audit trails and investigates thoroughly any security violations. Ensures audit trails are reviewed at least weekly and audit files are backed up.
- Ensures information systems or workstations are operated, maintained, and secured IAW AR 380-19 and unit SOP.
- Immediately reports any attempt to gain unauthorized access to sensitive defense information, any system failure, or any suspected defect that could lead to unauthorized disclosure. Also advises the S2 and/or security manager of security incidents or violations.
- Performs ISSO duties as prescribed in AR 380-19.

NETWORK SECURITY OFFICER (NSO)

A-6. The NSO ensures the secure interconnection of information systems on the LAN. The NSO–

- Controls LAN access.
- Monitors assigned LANs to ensure systems comply with security policies and applicable directives.
- Assists the ISSO in preparing, distributing, and maintaining security SOPs IAW AR 380-19.
- Conducts risk assessment reviews with the ISSO, ISSM, and functional proponent.
- Assists the ISSO in evaluating the security impact of changes to the network, including interfaces with other networks.
- Coordinates and monitors periodic security indoctrination and training sessions for assigned personnel.
- Ensures audit trails and other system management reports are reviewed for internal security audits or testing.
- Ensures information systems are operated, maintained, and safeguarded IAW AR 380-5, AR 380-19, and the SOP.
- Conducts specific security training for users, as required.
- Reports to the ISSO any attempt to gain unauthorized access to sensitive defense information, any system failure, or any suspected defect that could lead to unauthorized disclosure.
- Maintains a current access roster of persons with authorized access to all systems.

- Ensures users are aware of the requirement to verify security clearances before granting access privileges to information systems.
- Provides positive control of the information systems within the user's area of responsibility.
- Prevents unauthorized tampering of hardware or software.

SECURITY MANAGERS

A-7. Unit security managers are responsible for the information security programs within their organizations, and they directly support ISS personnel in executing security policies and procedures. Security managers–

- Are responsible for information (documents), personnel, and physical security.
- Ensure all personnel who use or have access to information systems have been screened IAW AR 380-67 and have a SECRET security clearance, as a minimum.
- Implement security directives in managing classified information.
- Act as the staff focal point for security issues.
- Distribute changes to policies and similar security-related information to the ISSOs.
- Process applicants for security clearances, verify security clearance status for users, and support personnel within their units.
- Prepare security clearance access rosters for the ISSOs.
- Establish annual security training programs for persons having continued access to classified information.
- Conduct security-related inspections throughout their units for compliance with security standards.

COMSEC CUSTODIANS

A-8. The commander appoints the COMSEC custodian. He is responsible for access and control of accountable COMSEC material. Information systems do not require any new or unique COMSEC material or controlled cryptographic items (CCIs). The COMSEC custodian–

- Incorporates procedures for operating, handling, and securing COMSEC material into local COMSEC procedures currently in effect, including periodic inspections.
- Trains users on handling, using, and safeguarding COMSEC material, including key lists and CCIs.
- Maintains accountability of all CCIs.

MISSION APPLICATIONS USER

A-9. The mission applications user–

- Complies with the security requirements in this SOP and applies directives for safe and secure operation.
- Has a SECRET security clearance, need-to-know, and training.

- Maintains positive physical control of information systems, as a high dollar value item, within their area of responsibility.
- Secures the system IAW AR 380-19 as SECRET material is processed and stored on its hard disks or floppy disks.
- Reports to the SA/NA or ISSO any security violation, attempts to gain unauthorized access to sensitive defense information, any system failure, or any suspected defect.

SECURITY REVIEW

A-10. Secure operation of information systems requires constant vigilance and attention in an ever-changing environment. Command and managerial personnel must periodically reassess the risks their specific operating environments present to the security of information systems. To assist in conducting a security review, the following subparagraphs focus on specific areas that should be reevaluated on a regular basis.

COMPLYING WITH THE GENERIC ACCREDITATION

A-11. Information systems will process classified information at the SECRET level. Commanders and ISS personnel are responsible for meeting the minimum-security requirements of the generic accreditation IAW AR 380-19. Commanders and ISS personnel can use a security checklist to determine if their unit is complying with the generic accreditation. (See Table A-1 at the end of this appendix.)

RISK MANAGEMENT

A-12. The entire ISS staff shares the responsibility for properly operating information systems. Each BFA is responsible for conducting threat and vulnerability assessments and reviews to help commanders assess the risks. These assessments and reviews are an essential part of the risk management process. Local commanders and ISS personnel need to consider the security environment in garrison, tactical situations, and all operating environments. Deployable information systems must be accredited to operate in a deployed environment. A risk analysis of the system will determine the environment in which the system will operate. Since conditions, including the environment and threat, change as computer systems deploy, the following factors must be considered for deployment.

Sensitivity

A-13. Sensitivity relates to the information being processed in a deployed situation, the classification level of equipment or information may increase based on the mission it supports. It should be possible to predict increased sensitivity before deployment by studying intelligence assessments and OPORDs the organization is tasked to support.

Criticality

A-14. Criticality relates to the mission the system supports or the degree in which the mission depends on the system. Criticality normally increases during deployment because of support to higher level commands and operational mission requirements. The user must determine what effect loss or alteration of the system or data would have on other systems and missions.

Password Management

A-15. The ISSO manages passwords used for access control as specified in AR 380-19. Users will not have any control over choosing their password. If passwords are used to determine need-to-know, classify them at the highest level of information that can be accessed; otherwise, protect as For Official Use Only (FOUO).

Physical Security

A-16. Physical security requirements usually increase as the sensitivity, criticality, and threats increase. The ISSO must access the increased sensitivity, criticality, and threat, then determine appropriate security measures. Physical security is an important part of the overall computer security plan during deployed operations. It includes controlling access to the computers and establishing a secure perimeter for the deployed site.

TEMPEST

A-17. The ISSO must carefully review TEMPEST requirements for deployed operations. Systems deployed to a hostile threat area may require increased TEMPEST countermeasures to meet the requirements of a countermeasure assessment. Coordination with the organization's TEMPEST officer is essential before and during a deployment to determine TEMPEST requirements.

Emergency Destruction

A-18. Deployment to medium or high threat areas dictates developing emergency destruction procedures for software, firmware, magnetic media, hardware, and hard copy output. The ISSO must consider equipment used, information processed, and anticipated time available for destruction to develop the best destruction method.

Risk Analysis

A-19. Deployable systems require a risk analysis package. The ISSO conducts a risk analysis of the system to describe a baseline environment. This environment should describe the minimum protection required for each state of operation. The security features of the system must satisfy the security requirements for the most restrictive environment. The ISSO performs an informal risk analysis at each deployed site to determine unique or additional protection.

Plans

A-20. The ISSO should help to develop plans for deployable information systems. These plans must address unique deployed operating conditions, such as temperature and humidity variations, power fluctuations, and dust. Plans needed for deployment include a security plan and the continuity of operations plan (COOP). The COOP should include emergency destruction and declassification procedures, backup procedures, alternate power sources, partial or degraded systems operation, and approved methods of disposal. The security plan should include a description of the baseline environment, additional safeguards for varying threats, and minimum operating conditions.

Backup Requirements

A-21. The ISSO investigates and documents system requirements for a possible hostile and stressful environment. System requirements will vary with different deployments and information systems. The ISSO must consider the task being automated, the mission criticality, and the deployed environment. He must also consider human factors if a manual backup is expected. Procedures for operating the manual and automated system should be similar, so transitions can occur quickly from the automated to the manual mode.

REVIEW OF SECURITY VIOLATIONS

A-22. A review of security violations must occur on a regular basis. The review will include all previous violations. The reviewer attempts to determine if any trends or patterns can be identified which may be of concern. The results of this analysis shall be incorporated into the risk management program and also be factored into the security training program assessment.

ASSESSING THE SECURITY TRAINING PROGRAMS

A-23. Security training programs should be evaluated periodically IAW AR 380-19. A successful training program must emphasize security fundamentals and contemporary security issues related directly to information systems. Both the initial security training program and the recurring training program should be revised to reflect the ongoing risk management effort and security violations review. The training program will also be reviewed and revised following the reaccreditation of information systems.

OPSEC

A-24. OPSEC procedures are based on the need to deny the enemy information about friendly capabilities and intentions. Commanders–

- Implement OPSEC procedures in this SOP.
- Comply with existing unit OPSEC procedures and related security procedures addressed in this SOP.

PHYSICAL SECURITY

A-25. Hardware, software, documentation, and data will be protected to prevent unauthorized disclosure, destruction, denial of service, or modification. Physical security is one of the principal means used to protect against these threats. AR 190-13 and FM 19-30 provide specific guidance on physical security requirements. Physical security at each site is based on an analysis of regulatory requirements, mission criticality, sensitivity levels of the information being processed, security threats, and the vulnerability of information systems to the security threats.

STORAGE AND SHIPMENT

A-26. The user must purge all information systems components IAW applicable technical manuals before shipping or storage. The user will remove all classified material and store it in a General Services Administration (GSA)-approved security container.

A-27. Requirements for protection can increase during storage or shipment due to increased vulnerability. Increased threat and vulnerability considerations include special handling requirements during shipment. Considerations include whether the system components would ever be out of US control at any time during shipment, and if stored, what protection is provided at the storage location.

A-28. After all removable classified media is removed and nonremovable media is purged, information systems must be provided double barrier protection. Information systems components will normally be stored in locked military vehicles or communications shelters within a locked building or fenced motor pool.

A-29. The storage locations of information systems equipment are included on the staff duty officer or charge of quarters security checklists.

ADMINISTRATIVE MOVEMENT

A-30. Before any move, all information systems components must be accounted for and placed in a proper configuration for movement IAW applicable technical manuals. During administrative movements, if classified material is resident on information systems components, an authorized individual must guard them.

A-31. If transported by unauthorized personnel, the CCIs must be provided double barrier protection during transportation. This can be accomplished by securing the components to the shelter with a locking cable, then locking the shelter, or by dismounting the component and storing it in a separate locked container in the locked shelter.

A-32. After the move, all components must be accounted for.

TACTICAL MOVEMENT

A-33. Before any move, all information systems components must be accounted for and placed in a proper configuration for movement IAW applicable technical manuals.

A-34. During movement, information systems will be protected IAW the level of classified information stored in them. Personnel will execute emergency destruction plans when an ambush, enemy contact, or capture of information systems and components is imminent.

A-35. After completing the move, all information systems components must be accounted for.

GARRISON OPERATIONS

A-36. During garrison operations, information systems must be protected IAW the classification of the data and COMSEC key that is in use. When FOUO data and key material are used, the user can provide adequate security for the system. If classified data or key material is used, the site requires additional security measures of a secured perimeter and a guard limiting access to authorized personnel.

A-37. No personnel shall be granted access to information systems simply because they possess the requisite security clearance or because of their duty position. Commanders will determine whether a person’s individual duties require access to information systems.

TACTICAL OPERATIONS

A-38. During tactical operations, information systems must be provided a secure site. Ideally, the site will have a perimeter fence and guards limiting access to authorized personnel. The minimum measure is an armed guard providing area security. System users must be aware of system security requirements at all times and provide at least the minimum security necessary. System users must enforce noise and light discipline in the site to minimize risk of compromise.

PERSONNEL SECURITY

A-39. Commanders, ISSOs, SAs/NAs, and users will enforce security procedures to limit access to unauthorized personnel.

A-40. Users will maintain positive control of information systems at all times. This includes restricting unauthorized personnel from observing the system's screen.

A-41. SAs/NAs and users will use access rosters and physical recognition to authorize access to information systems by other individuals.

MINIMUM CLEARANCE

A-42. All personnel operating C2/information systems WILL have a minimum of a SECRET security clearance.

NEED-TO-KNOW

A-43. The number of personnel cleared and granted access to the C2 networks will be kept to a minimum. No personnel will be granted access simply because they possess the requisite security clearance or because of their duty position. Commanders will determine whether a person's individual duties require access to the C2 network. Only authorized personnel should have access to the immediate areas where computers are operating.

A-44. Users will only have access to the information required to perform their assigned tasks, regardless of the user's security clearance. All commanders, assisted by their ISSOs, shall determine the maximum information access requirements of each user.

INITIAL TRAINING

A-45. All users are given initial security training. This training covers–

- Threats, vulnerabilities, and risks associated with the system.
- Reducing threats from malicious software.
- Prohibiting unauthorized software.
- Reducing the need for frequent backups.
- Reporting abnormal program behavior immediately.
- Information security objectives (what needs to be protected and why).
- Responsibilities associated with the system security.
- Information accessibility, handling, and storage considerations.
- Physical and environmental considerations necessary to protect the system.
- System data and access controls.
- Emergency and disaster plans.
- Authorized system configuration and associated configuration management requirements.

Ongoing Training

A-46. Security personnel will provide sustainment security training to users. Refresher training is conducted as needed. These updates should focus not only on those areas addressed in the initial security training, but also those areas that are discovered to be security risks based on the local risk assessment. Specific areas include–

- A review of security violations.
- New threats and associated countermeasures.
- Continuity of operations.
- Changes to security requirements.

A-47. All users, supervisors, and other personnel are trained to detect unauthorized or nonsecure procedures. Any person who detects or witnesses an unauthorized or nonsecure act will immediately notify the appropriate security personnel. This is true regardless of the rank of the person performing the nonsecure or unauthorized act or the rank of the person detecting the nonsecure or unauthorized act.

MAINTENANCE PERSONNEL

A-48. Maintenance personnel must be cleared to the highest classification level of data processed on the system. If this is not feasible, an individual with the required clearance and technical expertise will observe the maintenance personnel.

A-49. SAs/NAs will verify the security clearances of maintenance personnel before granting them access. The ISSO and the unit security manager will be notified BEFORE uncleared maintenance personnel are granted access or inadvertently gain access to classified information.

A-50. If components with classified information must be removed, the user will first purge the component. If the component cannot be purged, it will be stored in a GSA-approved security container until approved for release by the ISSO. Once cleared for release, maintenance personnel will be advised of the security classification and handling procedures of the classified material. Uncleared personnel will not remove classified components from the shelter.

INFORMATION SECURITY

A-51. Information security includes the measures taken to prevent disclosure, alteration, substitution, or destruction of data.

HANDLING CLASSIFIED MATERIAL AND INFORMATION

A-52. The guidelines for handling classified material and information are covered below.

A-53. All personnel will maintain positive control of all classified material for which they are responsible. Classified material will not be given to any individual who does not have the requisite security clearance and approved need-to-know.

A-54. Personnel carrying classified documents from the system's shelter to another location within the site perimeter must cover the material with a classified document cover sheet. Persons wishing to remove classified material from the site perimeter must wrap the material as directed by AR 380-5 and have DD Form 2501.

A-55. A system to provide accountability and control of classified material shall be established IAW AR 380-5. This system shall address creating, disseminating, and transferring classified information.

A-56. Handle and safeguard the printer ribbon IAW the classification of the material printed and AR 380-19.

MARKING PROCEDURES

A-57. All items being replaced or transported containing classified data will be marked IAW AR 380-19.

Removable Magnetic Media

A-58. All removable magnetic media shall bear external markings that clearly indicate the classification of the information.

A-59. SF 707 identifies removable media that contains information classified up to the SECRET level.

A-60. SF 710 identifies removable media that contains information that is unclassified.

A-61. SF 711 properly identifies the removable storage media. Use internal markings on files to indicate the classification and any special handling instructions. Mark in an obvious location all media used to store classified information. Mark the highest classification of data recorded on the media.

A-62. Personnel with a security clearance equal to or greater than the classification of the media shall only handle classified removable magnetic media.

Printed Material

A-63. C2 printer output will initially be controlled as SECRET material. As the operational situation permits, the material will be reviewed to determine the actual classification.

A-64. After manually reviewing printer output, it will be marked with the correct classification, classification source, and declassification date. As a reminder, this is not downgrading classified information, but only appropriately labeling.

Printer Ribbons and Toner Cartridges

A-65. Printer ribbons and toner cartridges will be marked with the same classification level as the material printed.

STORAGE PROCEDURES

A-66. All classified material will be stored in GSA-approved security containers when not in use by appropriately cleared personnel.

A-67. When one-drawer field safes are used to store classified material, the safe will be securely fastened to the shelter or guarded to prevent theft. Guards employed for this function only, and who do not otherwise have access to classified material, do not require a security clearance.

DESTROYING PRINTED MATERIAL

A-68. AR 380-5 provides guidance for destroying classified material associated with the TI. The secure-volume concept is the routine destruction of classified (paper) material originating from the printer. This concept stresses destroying at least 20 pieces of paper at a time. This results in an increased volume of residue. If necessary, add a sufficient number of unclassified pages to the classified document to arrive at the minimum 20-sheet page count.

A-69. If shredders are used for paper waste, ensure they are rated Class I (crosscut) or Class II (continuous strip).

A-70. When a shredder is not available, burning will destroy printed material. The fire must be carefully controlled to prevent burnt fragments that are still legible from being blown away. After all the material is burnt, wet and stir the ashes to destroy any legible burnt fragments.

A-71. Burning will destroy classified printer ribbons and floppy disks. When burning floppy disks, take precautions to avoid the toxic fumes that may be released.

A-72. Removing the platen and rollers and sanding the surfaces that contact the paper will destroy classified toner cartridges.

CLEARING, PURGING, DECLASSIFYING, AND DESTROYING ELECTRONIC AND MAGNETIC MEDIA

A-73. When information systems components are stored or left unattended, all classified information must be removed. Information systems components will have information stored in several locations.

A-74. The first is random access memory (RAM). RAM is very perishable and usually not accessible to the user once power has been removed. However, purge procedures addressed in this SOP must be followed to ensure classified data is removed.

A-75. The second location is components that have a permanent storage capability. The memory of these components is usually not affected by the removal of power. Procedures in this SOP must be followed to ensure classified data is properly protected.

A-76. Clearing of media means erasing or overwriting all information on the media, but without the totality and finality of purging. Removable media that has simply been cleared must continue to be controlled at their prior classification or sensitivity level.

A-77. Purging of media means to erase or overwrite totally and unequivocally any information stored on the media.

A-78. Declassifying of media refers to the administrative action taken after it has been purged. Declassify media for storage and shipment to reduce the amount of control and protection required. If the media contains classified software or data, copy it to removable media, if possible. If the ISSO cannot declassify the media, control and protect it as classified equipment.

A-79. Use overwrite procedures to purge classified data before storage or shipment. Once the data has been purged, the appropriate declassification authority must document the final decision to remove the classification from the media. Unless there is a hardware device that prohibits writing to the hard disk, classify and protect the hard disk at the highest classification processed until purged. Transferring classified information from hard disk to floppy, or deleting a file, does not purge the hard disk. It remains classified until purged. Information systems that have nonvolatile, non-removable semiconductor memory cannot be purged. If these systems have processed classified information, they must be protected as classified equipment.

Removable Hard Disk

A-80. Declassifying using the same procedures as with a fixed-hard disk.

Monitors

A-81. Inspect monitors for burned-in classified images on the screen before packing for deployment. If any part of the screen retains classified information, treat the monitor as classified and protect accordingly. Safeguard computer hardware while deployed to prevent alteration or damage to the equipment.

Hard Disks

A-82. Protect hard disks as classified if they are mounted on or are in systems that process classified information unless there is a hardware device that prohibits writing to the hard disk. Transfer of classified information from the hard disk to a floppy, or deleting a file, does not purge the hard disk. The disk is still classified and requires protection until purged.

RAM

A-83. The RAM of the FBCB2, tactical multinet gateway (TMG), NMT(B2), and NTDR RAM is considered classified. This RAM will be purged when the component has been properly powered down and all power has been removed. No additional on and/or off cycle is required. To purge the RAM from the printer, the user will turn the printer off, wait 60 seconds, turn the printer on, wait for its memory test to run, then turn it off.

Permanent Storage

A-84. Floppy diskettes cannot be purged. Due to their low cost, diskettes will be destroyed when no longer needed.

A-85. Using the C2P-NSM tools to overwrite every storage location on the disk will purge the FBCB2, NMT(B2), and lightweight computer unit (LCU) hard disks. Because some storage locations on disks with bad sectors cannot be overwritten, they cannot be purged; therefore, they must be treated and safeguarded as SECRET material. The system workstation hard and floppy disks must be removed from the workstation and stored in a GSA-approved security container or class B vault or guarded by an authorized individual. AR 380-5 contains specific storage sites for classified media.

A-86. The COMSEC key material stored in EPLRS with a very high-speed integrated circuit (EPLRS VHSIC) and the SINCGARS SIP equipment is cleared by using the zeroize key on the radio while the power is on.

COMPROMISE

A-87. Situations involving known or suspected loss of classified information will be investigated to determine their cause. Cost-effective corrective measures will be implemented to prevent recurrence.

A-88. Suspected or actual security incidents will be reported to the SA/NA and ISSO by the fastest means available.

A-89. Incidents that may signal the beginning or presence of a possible security incident include–

- Unexplained output received at a terminal or from a printer.
- Extraneous data.
- Abnormal system responses.
- Any indication of media manipulation, modification, or corruption of files and data.

A-90. The ISSO will report security incidents not directly attributed to administrative error (such as system penetration, malicious acts by an operator, and so on) within five days, through the chain of command, to the Commander, United States Army Intelligence and Security Command (INSCOM), ATTN: IAOPS-CI-TO, Fort Belvoir, VA 22060-5370.

EMERGENCY DESTRUCTION PROCEDURES

A-91. Every effort should be made to prevent loss or compromise of the data processed by automated equipment.

A-92. When C2 or information systems equipment is subject to imminent danger or capture, the following actions will take place:

- Zeroize COMSEC material and destroy SOI, authentication codebooks, and any other hard-copy classified material.
- Purge the system workstation computer RAM and printer.
- Destroy equipment in the following order:
  - COMSEC devices.
  - Hard disks.
  - Floppy disks.
  - AN/UYK-86 computer.
- Destroy all information systems components to deny the enemy any use of the information or equipment.

- Disassemble and destroy the hardware, as much as possible, and burn it using petroleum, oils, and lubricants. If tools are not available, thermite grenades will be ignited directly over equipment, as needed.
- Integrate the emergency destruction requirements into the unit's tactical SOP and overall priority of the unit's destruction plan.
- Conduct dry runs and/or practices on a periodic basis.

COMSEC

A-93. The quality of information shared on the network is everyone's responsibility beginning at the user level. COMSEC includes clearances and most importantly the need-to-know. The G6/S6 and the ISSO are responsible to the commander for COMSEC IAW AR 380-19.

COMSEC EQUIPMENT AND KEY LISTS

A-94. The equipment used in ABCS uses many concepts and systems for generating, distributing, and managing electronic COMSEC keys. ABCS ensures the integrity and security of communications up to the SECRET level. ABCS considers the security of COMSEC material used by existing training material and unit SOPs regarding COMSEC handling.

A-95. Access to classified COMSEC material may be granted to US citizens whose duties require access. Security clearance requirements for persons granted access is determined by the classification level of the material to be accessed.

A-96. The G6/S6 will ensure COMSEC is–

- Distributed and implemented on a timely basis.
- Properly reported when lost or compromised.
- Properly disposed of or destroyed.
- Documented after destruction.

ELECTRONIC EMANATIONS

A-97. Compromising emanations are unintentional intelligence-bearing signals. If intercepted or analyzed, these signals will disclose unclassified sensitive and classified information transmitted, received, handled, or otherwise processed by information systems. Users will–

- Maintain and operate information systems.
- Check terminal cables periodically to ensure connections are in place.
- Report and have repaired any damaged equipment.

LAN

A-98. Data transmissions over a LAN must be protected in the same manner as transmissions over a radio. If the entire LAN resides within the confines of a physical control zone (PCZ), unencrypted transmissions over the LAN are considered protected.

A-99. When a LAN does not reside entirely within a PCZ, the LAN must be made a protected distribution system (PDS). Commanders may approve a PDS in a tactical environment. Under battlefield conditions, commanders may delegate this authority to company commanders. AR 380-19 discusses the use of a PDS.

A-100. The G6/S6 will verify that all LAN cables are properly tagged IAW unit SOPs.

SOFTWARE SECURITY

A-101. Software security depends on the prompt identification and resolution of all software errors. All software errors, no matter how insignificant, shall be reported so they may be investigated and corrected.

SOFTWARE ERRORS

A-102. AR 380-19 requires that information systems software be rigorously tested before approved for use. Despite the extensive testing efforts made before fielding, some software errors will undoubtedly occur. These errors, which may compromise security, must be properly addressed to preserve the protection provided by the software suite.

A-103. All users are responsible for promptly reporting software errors and abnormal or unusual system responses to the SA/NA, ISSO, or other point of contact (POC) IAW with unit SOP.

A-104. The following guidelines will protect software during storage and shipment from loss, damage, or alteration.

- Classification of the software determines the protection required.
- Software is stored away from high-voltage and magnetic material.
- Ship classified software separate from hardware using an approved storage container.
- Software contains proper internal and external security markings.
- Software receives the same level of protection in deployed operations and the home environment.
- Backup copies will have the same level of protection as the original.

VIRUSES

A-105. Computer viruses are rarely distributed with authorized system software. However, personal software has a much higher probability of contamination since it is not as tightly controlled. Entertainment programs and programs on electronic bulletin boards are ideal carriers for viruses and Trojan horses, since they are frequently copied and widely distributed. Programs of this nature WILL NOT be loaded on the computers.

UNAUTHORIZED SOFTWARE

A-106. The delivered software, as identified in the ABCS generic accreditation, has been authorized for use on ABCS after extensive testing and evaluation. The authorized software suite is an integral part of the ABCS security plan. Users are encouraged to make full use of the features and capabilities provided in these programs to accomplish their assigned tasks to preclude unauthorized actions.

A-107. Data files may be transferred between workstations on removable media IAW operating and security procedures to update necessary operating data.

A-108. Users WILL NOT load additional software programs other than authorized updated revisions.

A-109. AR 710-2 requires original copies of all software, regardless of value, to be issued and accounted for through normal hand-receipt procedures. Unit commanders will ensure that the software suite issued with each workstation is properly accounted for and hand receipted. The G6/S6 or ISSOs will ensure the compliance of copyrighted software licensing restrictions.

SOFTWARE MODIFICATIONS

A-110. Modification or alteration of the ABCS software is strictly prohibited. Only formally released software revisions or modifications shall be installed.

SOFTWARE INTEGRITY

A-111. The procedures set forth in this SOP are only effective if the integrity of the ABCS software is maintained. The G6/S6 or ISSO is responsible for the integrity of the ABCS software suite.

SYSTEM AUDIT PROCEDURES

A-112. Systems operating in the systems high mode of operation will ensure all persons having access to the system are held accountable for their actions. In the ABCS environment, this is accomplished through an audit trail. Because the ABCS software does not provide an automated audit trail of all security-related events, this tracking is done manually. Therefore, it is necessary for users to maintain a manual record of all security-related events.

A-113. As a minimum, an audit log will be reviewed daily for security implications. If the tactical situation does not permit the daily review of the audit log, commanders may authorize the review of the audit log weekly. Audit trail information will be maintained for 30 days.

CONFIGURATION CONTROL

A-114. The configuration of ABCS shall be strictly controlled. Proper configuration management practices play a significant role in preserving system security and in assuring continued performance.

A-115. Unit personnel will conduct regular inventories of information systems components. In addition to regular inventories, periodic inspections shall be conducted to verify the hardware configuration has not been altered. Each piece of hardware shall be visually inspected for signs of unauthorized modification or tampering.

A-116. An accurate accounting of all hardware shall be maintained throughout the system's life. This inventory shall reflect any authorized equipment replacements, upgrades, modifications, and additions that take place.

HARDWARE SECURITY

A-117. Hardware security depends on the prompt identification and resolution of all hardware errors. All hardware errors, no matter how insignificant, will be reported so they can be investigated and corrected.

HARDWARE MALFUNCTIONS

A-118. Although the hardware is thoroughly tested before fielding, some malfunctions will undoubtedly occur. It is important that these malfunctions be identified and corrected as quickly as possible. Malfunctioning hardware may undermine procedural or automated security features and make ABCS susceptible to unauthorized access attempts.

A-119. All users are responsible for identifying and reporting any equipment malfunctions so appropriate corrective action can be taken. Users can quickly resolve most equipment malfunctions that are caused by user errors.

A-120. Users identify most equipment malfunctions when they fail to receive the equipment response anticipated by an initiated action. Normally, after several unsuccessful attempts, the user will begin to look for an explanation of the equipment malfunction. The user will verify–

- The power is available to the device in question and cables are connected.
- All data is correct and has been properly input and the proper procedures were used.
- The built-in-test (BIT) is monitored during system initialization.
- Any equipment malfunction that affects the security.
- Local maintenance is conducted IAW the appropriate technical manuals and unit SOP.

EQUIPMENT INSTALLATION

A-121. The security of the system depends on the installation of the hardware suite. It is critical to the security and operation of the system that components are kept in their proper installation configuration.

SECURITY BRIEFING

A-122. AR 380-19 states that all users, supervisors, and managers of information systems receive initial and periodic training in automation security. This briefing fulfills the training requirements of AR 380-19. All personnel will read or will be briefed on this information. They will also acknowledge receipt of the briefing with their signature.

PURPOSE OF AUTOMATION SECURITY

A-123. ABCS and other information systems operate in the active Army, Army Reserve, and National Guard processing classified and unclassified sensitive information. These systems are vulnerable to computer hackers, hostile intelligence agents, thieves, and individuals with malicious intent. The rapid increase in information systems has made security a major issue concerning the safeguarding of systems and, most important, the data they process. The US Army Information Systems Security Program defines various threats to our information systems and applies countermeasures. The program protects against–

- Espionage.
- Compromise or unauthorized manipulation of classified and unclassified sensitive information.
- Unintentional loss or malicious destruction of data files.
- Malicious or unintentional damage to, or destruction of, hardware and software.
- Theft of hardware and software.
- Unauthorized use of software that may contain malicious programs (computer viruses, logic bombs).
- Unauthorized personal use of the equipment.
- Natural disasters.

PERSONAL RESPONSIBILITY

A-124. Users, supervisors, and managers must adhere to prescribed security policies and procedures. These are divided into three areas: procedural, data, and physical security, which constitute the minimum for operating the system.

PROCEDURAL SECURITY

A-125. Procedural security dictates how to operate and maintain the system. Users, supervisors, and managers will–

- Have a minimum of a SECRET security clearance and approved need-to-know.
- Obtain an information systems briefing from their ISSO or designated representative.
- Ensure the equipment and processing environment is maintained with care (for example, used properly and kept clean).

- Operate the equipment IAW operator's manuals and posted security instructions.
- Ensure that personal copies of software are not used on government equipment.
- Ensure that no additional equipment is attached to the network without the knowledge and permission of the ISSO. Attaching additional equipment will require additional accreditation.
- Protect against disaster (always have backup copies of programs ready to go).
- Protect unattended workstations.
- Protect against viruses (never load unauthorized or personal software onto any workstation).
- Report immediately any suspected computer misuse or abuse to the ISSO.

DATA SECURITY

A-126. Always protect classified and unclassified sensitive information. Sensitive and mission critical information requires protection from disclosure, alteration, and loss. Classified data products must be safeguarded (processed and stored) IAW AR 380-5. Users, supervisors, and managers will–

- Protect data storage media (secure removable media and equipment that contain fixed media).
- Not attempt unauthorized access to any data on any ABCS equipment or network.
- Label disks with the contents of the data stored on them (classified and unclassified) and the name of the application program.
  - Handle disks carefully to avoid damage.
  - Do not write on a disk with pencil or pen. (The correct procedure for labeling a disk is to write the classification and identification data on the label and then attach the label to the disk.)
- Label disks used for classified data with the highest classification of the information contained on the disk. (Use SF labels for SECRET and unclassified, when appropriate.)
- Store classified and unclassified disks in jackets that have been correctly labeled.
- Mark classified data output products at the top and bottom of the page with the proper classification and required caveats IAW AR 380-5.
- Verify that all output (hard copy, files, and media) are marked with the proper classification.

- Dispose of waste containing classified information as classified waste (for example, burn or shred).
- Not allow any person outside the organization to access information unless the person has a SECRET security clearance and a need-to-know.
- Store classified and sensitive data products in authorized security containers IAW AR 380-5.

PHYSICAL SECURITY

A-127. Physical security limits access to the processing environment and provides security for hardware, software, and the data it processes. Users, supervisors, and managers will–

- Protect data processing areas (recognize people who do not belong in the area).
- Limit access to those who are authorized to use, service, and repair the equipment.
- Lock doors to offices, rooms, vehicles, and motor pools that house information systems during nonduty hours.
- Restrict access to areas where classified information is being processed.
- Ensure that hardware and software are hand receipted by serial numbers to users, sections, or office chiefs. Hardware and software must have an accountability chain back to the property book officer.
- Challenge persons carrying components out of an office, building, motor pool, or net control station (they may be in the process of stealing).
- Not allow storage media, on which classified and/or unclassified sensitive data or applications has resided, to leave controlled channels until it has been declassified.

PERSONAL LIABILITY

A-128. Users, supervisors, and managers must know the Federal law provides for punishment of up to a $100,000 fine and one year in jail for the first offense of anyone who–

- Knowingly accesses a computer without authorization or exceeds authorized access and obtains information which requires protection against unauthorized disclosures.
- Intentionally accesses government-owned computers without authorization and alters, damages, or destroys information or prevents authorized use of the computer.

A-129. The offense is for the access and not necessarily disclosure.

ACKNOWLEDGMENT

A-130. Users, supervisors, and managers will acknowledge, by signature, that they have read and understood the above instructions. The ISSO or SA/NA (briefer) must answer any questions regarding these instructions before signing. Persons who refuse to acknowledge the briefing will not be allowed to operate in the network. All persons receiving this briefing will be given a signed personal file copy for future reference.

USER: ______________________________RANK: _________DATE: ____________

ISSO: ______________________________RANK: _________DATE: ____________

TECHNICAL VULNERABILITIES

A-131. This section describes policies and procedures for reporting technical vulnerabilities (for example, contamination and intrusions and/or attempted intrusions).

A-132. A technical vulnerability is a hardware, firmware, communication, or software weakness that is not documented in the system's literature. It leaves a computer processing system open for potential exploitation, either externally or internally, resulting in a security risk.

A-133. Some technical vulnerabilities include–

- The use of software commands which unexpectedly disable protection features.
- The failure of the hardware to separate individual processes or to protect security relevant protective mechanisms from unauthorized access or modification.
- A communications channel which allows two cooperating processes to transfer information such that the transmission violates the system's overall security policy.

RESPONSIBILITIES

A-134. The ISSM–

- Serves as the commander's representative on ISS.
- Maintains a technical threat database on technical vulnerabilities, such as contamination and intrusion attack methodologies, and provides this information to individuals on a need-to-know basis.
- Provides security training to educate users about the threats of technical vulnerabilities. This ensures the users are aware of defensive strategies, which may be taken to control and minimize threats and to advise users of reporting requirements under Federal statute and Army directives.

A-135. The ISSO–

- Reports any security incidents and technical vulnerabilities to the higher headquarters ISSO or ISSM.
- Implements automation security training to include technical vulnerability reporting.
- Provides support to the ISSM and to the INSCOM, as necessary.

A-136. Users will–

- Comply with AR 380-19 and the unit SOP.
- Immediately report any suspected or actual security violations, such as contamination, intrusions and/or attempted intrusions, and other technical vulnerabilities, upon their detection, to their SA/NA or ISSO.

POLICIES

A-137. All computer contamination, intrusions and/or attempted intrusions and other technical vulnerabilities will be reported immediately upon their detection to the SA/NA or ISSO.

A-138. As a minimum, all information on technical vulnerabilities will be classified at the CONFIDENTIAL level. Individuals reporting such information must use a secure means of transmission and ensure that the recipients of the transmitted information have the proper security clearance and need-to-know. If the individual reporting the information does not have access to a STU-III security phone (or other COMSEC device), the ISSO or ISSM should be notified in person, or by mail, regarding the technical vulnerability information.

A-139. All technical vulnerabilities will be reported IAW AR 380-19.

A-140. IAW AR 380-19, vendors may be provided with the technical details of vulnerabilities. Within contractual limitations, the prime contractor is responsible for taking corrective actions and for establishing procedures that will eliminate identified technical vulnerabilities.

A-141. Same day reporting to the INSCOM is required for actual intrusions, virus attacks, or other events which would likely affect or apply to other sites.

PROCEDURES

A-142. Audit trail records are an essential element of detecting a technical vulnerability. Information systems components will be audited IAW the standards of AR 380-19 and the unit SOP.

A-143. Users will report suspicious activities to their SAs/NAs or ISSOs for a determination on whether a security incident or technical vulnerability has occurred and what action must be taken. Suspicious activities include–

- Successful and unsuccessful connections from external interfaces that do not normally establish connections to the network.
- Alert messages, which indicate that users have attempted to execute or obtain privileges that they have not been granted.
- Unauthorized use of the network.

A-144. If the vulnerability is a possible contamination, the component or system should be isolated from other components. Disconnect the system, if necessary.

A-145. The SA/NA, with assistance from the ISSO, will attempt to identify contamination symptoms which may be present based on a baseline of normal system operation.

A-146. Technical vulnerabilities will be reported immediately. Individuals will contact their SA/NA or ISSO for the initial reporting of the vulnerability. If the SA/NA or ISSO is not available, contact the ISSM.

A-147. The format for reporting a technical vulnerability will be IAW AR 380-19. The report should be thorough and detailed so the vulnerability can be demonstrated and researched.

A-148. All reports of technical vulnerabilities will be initially classified at least CONFIDENTIAL. The INSCOM, with the National Security Agency, determines if the report should be declassified to facilitate dissemination.

A-149. ISSOs will investigate the validity of all possible technical vulnerabilities, including contamination and intrusions and/or attempted intrusions.

A-150. ISSOs will coordinate technical recovery actions based on guidance from their ISSM and ISSPM and will submit interim and final reports on all vulnerability incidents.

A-151. If an ISS incident occurs because of a technical vulnerability, the security incident and the technical vulnerability can be combined on the same report IAW AR 380-19.

REPORTING

A-152. A report must contain general information. This includes–

- Report date.
- Person(s) contacted (include person's position, organization, mailing address, and telephone number).
- Hardware and software configuration, including the operating system (with release number) and any unique attributes, such as special security properties.
- Description of a technical vulnerability that includes–
  - A scenario that describes the specific conditions which demonstrate the weakness or design deficiency. The description should thoroughly describe the condition(s) so the deficiency can be demonstrated and researched with the given information.
  - A description of the specific impact or effect of the weakness or design deficiency in terms of denying service, altering information, and compromising data.

  - An indication of whether or not the vendor has been notified. The prime contractor may be provided with the technical details of vulnerabilities to take corrective actions within contractual limitations IAW AR 380-19. The vendor should not be provided with data regarding the specific sites concerned, methods of discovery, or information that could lead to increased site vulnerabilities without the written approval of the DAA.
  - A suggested correction. Any code or procedure that will reduce the impact or eliminate the defined technical vulnerability.

- System location, owner, network connections, system use, highest classification of data, and any other clarifying information. See Table A-1 for the security checklist contained in this SOP.

SECURITY CHECKLIST

A-153. Table A-1 is a security checklist that provides the information needed to ensure the unit is operating the equipment IAW AR 380-19 and unit SOP.

Table A-1. Security Checklist

Unit Identification: ______________________________

Number of System Workstations:______________________________

Unit Location: ______________________________

ISSO:______________________________

SA/NA:______________________________

Unit Security Manager's:______________________________

Name/Title:______________________________

Telephone:______________________________

Supervisor's Name/Title:______________________________

Telephone:______________________________

YES	NO	ACCESS
□	□	All personnel have a minimum of a SECRET security clearance.
□	□	Access rosters for all information systems. (Once the security clearance and the need-to-know are verified, access is granted.)
□	□	All systems connected to the LAN are properly accredited.
YES	**NO**	**AUDIT**
□	□	C2P tools are used to capture audit events.
□	□	Audit tools are reviewed for evidence of unauthorized access or tampering.
YES	**NO**	**CLEARING, PURGING, AND DECLASSIFYING ELECTRONIC MEDIA**
□	□	When left unattended, the information systems components must be placed in a purged, declassified state. All classified magnetic media is removed; workstation RAM is purged; and printer RAM is purged.
□	□	Floppy disks with classified information stored on them are always treated as classified and not used at the unclassified sensitive level. (Floppy disks can only be purged using a Type I or II Degausser.)

Table A-1. Security Checklist (Continued)

YES	NO	HARDWARE SECURITY
□	□	All information systems components are installed and maintained IAW applicable technical manuals.
□	□	All information systems component failures or malfunctions are documented and reported to the SA/NA or ISSO. (ISSOs will determine if the malfunctions should be reported as a technical vulnerability.)
□	□	Maintenance personnel have a SECRET security clearance.
□	□	Maintenance personnel with no SECRET security clearance and who do not access classified information during their operations are observed by an authorized individual with a SECRET security clearance, to ensure they perform no obvious unauthorized modifications.
□	□	Classified information systems components are not removed from the shelter by uncleared maintenance personnel.
YES	**NO**	**SOFTWARE SECURITY**
□	□	System workstation software errors or failures are documented and reported to the SA/NA or ISSO. (ISSOs will determine if software errors should be reported as a technical vulnerability.)
□	□	No unapproved modifications or alterations are made to the system workstation software.
YES	**NO**	**PHYSICAL SECURITY**
□	□	When unattended, the information systems components are secured with double barrier protection (for example, locked in a military vehicle or in a locked and secured motor pool).
□	□	Environment for operating information systems is authorized for processing SECRET material.
□	□	All components are maintained under the control of cleared, authorized users or supervisors.
□	□	Classified information, magnetic media, and other material are secured in a GSA-approved container, safe, or Class B vault when not under the direct control of an authorized individual.
□	□	All components are properly declassified before being left unattended.

Table A-1. Security Checklist (Continued)

YES	NO	PROCEDURAL SECURITY
□	□	ISSO is appointed.
□	□	Missions applications administrator assists SA/NA and ISSO in accomplishing security.
YES	**NO**	**PERSONNEL SECURITY**
□	□	Initial security training and awareness briefing for all workstation users and supervisors is given.
□	□	Periodic security and awareness training program is given.
□	□	All personnel who have access to the network have a minimum of a SECRET security clearance IAW AR 380-67.
YES	**NO**	**INFORMATION SECURITY**
□	□	All workstation removable magnetic media is clearly marked to indicate the classification of information stored on it (SF 707 or SF 710 label).
□	□	All workstation printer output is marked and safeguarded as SECRET until reviewed and marked accurately by an authorized individual.
□	□	Printer ribbons used by the workstation to print classified information are marked and stored with appropriate classification level.
□	□	All classified material, documents, removable magnetic media, printer output, and COMSEC material are secured in a GSA-approved container for securing classified material, a Class B vault, or guarded by an authorized individual.
YES	**NO**	**EMERGENCY DESTRUCTION**
□	□	Procedures to destroy workstations to prevent compromise of classified and unclassified sensitive information are in place.
□	□	Emergency destruction procedures are in place during tactical movements.
□	□	Emergency destruction procedures are periodically rehearsed.

Table A-1. Security Checklist (Continued)

YES	NO	TRANSPORTATION SECURITY
□	□	Procedures are in place to protect all components during tactical movements.
□	□	Procedures are in place to protect all components during administrative movements.
YES	**NO**	**MISCELLANEOUS**
□	□	AR 380-19 is on hand.
□	□	Unit SOP is on hand.
□	□	The command has conducted a local risk management review.
□	□	POC list for SA/NA, ISSO, and ISSM is on hand.